A Security Argument Pattern for Medical Device Assurance Cases

Anita Finnegan, Fergal McCaffery
Regulated Software Research Centre
Dundalk Institute of Technology
Dundalk, Ireland
{anita.finnegan, fergal.mccaffery}@dkit.ie

***Abstract*—Medical device security is a growing concern for medical device manufacturers, healthcare delivery organisations and regulators in the industry. Increasingly, researchers are demonstrating exactly how vulnerable these devices are. In many cases, networked medical devices are regarded as a potential weak link within a healthcare IT network that could provide a means to expose the entire network to a malware attack. At present there is no formal method for implementing security risk management practices in the medical device industry. However, with new regulatory guidance being developed by the Food and Drug Administration (FDA), medical devices manufacturers will need to prove that their devices are secure. This paper presents a security case framework that is currently under development. The purpose of this framework is to provide medical device manufacturers and healthcare delivery organisations with a solution to assist both in establishing confidence in the security assurance of medical devices and to also maintain this confidence throughout the lifetime of the device.**

Keywords—assurance cases; security cases; medical device security; cybersecurity; security capability argument pattern.

I. INTRODUCTION

Over the past few years the use of interoperable and networked medical devices has increased dramatically. These medical devices have functionality to communicate via healthcare IT networks in a variety of different ways i.e. wirelessly, across the internet, and from device to device. With this increase in adoption and availability of interconnected medical devices, patients can now receive around-the-clock care, outside the healthcare environment, and even in the comfort of their own home. Consequently, resource demands to administer this patient care is significantly reduced. Healthcare delivery organisations utilize a wide range of networked medical devices from hard-wired monitoring devices such as diagnostic equipment (CT scanners) to implanted medical devices such as defibrillators. The benefits of networking these devices are significant but in using such technology, a new set of risks arise which can impact the safety of a patient. These are security risks, threats and vulnerabilities.

Until now medical device manufacturers have only been required to demonstrate that their device is safe and effective. With the upcoming FDA cybersecurity regulatory guidance, manufacturers will now have to demonstrate that a medical device is also secure prior to placing it on the market [1]. In order to satisfy this requirement, it is recommended that manufacturers supply documentation detailing (1) the security risks identified during the design stage, (2) the security controls and justification of these controls to mitigate the risks, and (3) a traceability matrix linking the security controls to the security risks.

This paper describes research being conducted to develop a framework to meet the requirements of this regulatory guidance through the use of assurance cases. Assurance cases are structured, evidence based arguments used to demonstrate confidence that a system holds a particular critical property. Assurance cases were originally used to address safety concerns for systems but the use of assurance cases has grown exponentially. Consequently, assurance cases are currently used to address other critical properties such as dependability, reliability and security across a range of safety critical domains such as automotive, railway, defence, aviation etc. Whenever assurance cases are used to argue safety and dependability they are referred to as safety cases and dependability cases respectively. Similarly, an assurance case arguing the security of a system/software is called a security case.

Traditionally, assurance cases in the medical device domain have been used to address safety concerns [2]. Since April 2010, Infusion Pump manufacturers have been operating under the Infusion Pump Improvement Initiative where a draft guidance document [3] recommends the use of assurance cases for use during the approval process for new Infusion Pumps entering the market. The FDA recommends the use of assurance cases to communicate information about the safety of the device and how risks have been identified and mitigated [3]. The objective of the research is to investigate how a security case framework can be adopted by both medical device manufacturers and healthcare delivery organisations to improve the overall security practices during both device development and operation, right through to retirement.

II. Overview

This framework leverages on a number of security related standards [4], [5], [6], [7], [8], [9], [10] and utilises the concepts of Goal Structure Notation (GSN) and an argument pattern [11]. In this particular instance, security cases are intended to demonstrate confidence in the establishment of security capabilities (as outlined in IEC/TR 80001-2-2). It is difficult to argue that a system is secure [12] [13] beyond all doubt. Therefore, a more obtainable approach has been employed which argues that a number of security capabilities have been acceptably established using a risk based approach.

IEC/TR 80001-2-2 - *Application of risk management for IT-networks incorporating medical devices - Guidance for the communication of medical device security needs, risks and* controls is a technical report which aims to promote the communication of security controls, needs and risks of medical devices to be incorporated into IT networks between medical device manufacturers, IT vendors and healthcare delivery organisations. This is the only guidance available to medical device manufacturers and healthcare organisations that specifically addresses security requirements for networked medical devices. The technical report presents an informative set of high level security capabilities which are intended to be the starting point for discussion between stakeholders. There are a total of 19 security capabilities (see Table I) which provide a template for a healthcare organisation to communicate their security requirements for a given medical device based on their needs taking into account operational environment, network infrastructure, interconnected devices, users etc. The aim is to facilitate more effective communication of the security requirements for a medical device. IEC/TR 80001-2-2 security capabilities are the foundation of this framework.

Table I - IEC/TR 80001-2-2 security capabilities

Code	Security Capability	Code	Security Capability
ALOF	Automatic logoff	MLDP	Malware detection/prevention
AUDT	Audit Controls	NAUT	Node Authentication
AUTH	Authorization	PAUT	Person Authentication
CNFS	Configuration of Security Features	PLOK	Physical Locks on Device
CSUP	Cyber Security Product Upgrades	SGUD	Security Guides
DTBK	Data Backup and Disaster Recovery	SAHD	System and Application Hardening
EMRG	Emergency Access	RDMP	Third-Party Components in Product Lifecycle Roadmaps
DIDT	Health Data De-Identification	TXCF	Transmission Confidentiality
IGAU	Health Data Integrity and Authentication	TXIG	Transmission Integrity
STCF	Health Data Storage Confidentiality		

The security capabilities are intended to support the maintenance of confidentiality, integrity and availability which may otherwise be compromised intentionally or unintentionally. IEC/TR 80001-2-2, defines a security capability as "*a broad category of technical, administrative and/or organisational security controls required to manage risks to confidentiality, integrity, availability and accountability of data and systems*". The security capabilities do not however provide sufficient detail for the specification of requirements but instead provide a classification and structure that can be used to organise such requirements [4]. A key component of this research was to determine how such security capabilities could be established through the implementation of a set of existing security controls. For this reason, the following security standards we selected (based on expert opinion) to identify these categories of security controls required to establish each of the security capabilities:

- ISO 27799;
- ISO/IEC 27002;
- IEC 62443-3;
- NIST SP 800-53;
- ISO/IEC 15408-2;
- ISO/IEC 15408-3.

All relatable controls from each of the six standards were mapped to the 19 security capabilities. This work (lead by the authors and validated by the international medical device standards working group IEC SC62a JWG7) is currently at a committee draft stage and expected to be published as IEC/TR 80001-2-8 [14] with the International Standards Committee IEC SC62a JWG7. This document presents the categories of security controls prescribed for a system to establish security capabilities to protect the confidentiality, integrity, availability and accountability of data and systems.

The security controls support the maintenance of confidentiality and protection from malicious intrusion both of which could potentially lead to compromises in integrity or system/data availability. An example of one of the security capabilities (automatic logoff -ALOF) and associated, mapped security controls is presented in Table II. Table II illustrates that there are a total of 25 technical, administrative, operational and management security across all 5 standards for ALOF. The selection of security controls for each security capability will be dependent upon the medical devices manufacturers': defined acceptable risk tolerance; required rigour; preferable security standard/guidance resource; and the appropriateness of the security control etc. [15].

Table II - Security controls for automatic logoff (ALOF)

Standard	Ref	Control
SP 800-53	AC-1	Access Control Policy and Management
	AC-11	Session Lock
	AC-12	Session termination
	IA-11	Re-authentication
ISO/IEC 15408-2	FTA_SSL	Session Locking and Termination
	FMT_SAE	Security Attribute Expiration
	FIA_UAU	User Authentication
ISO/IEC 27002	5.1.1	Policies for information security
	5.1.2	Review of the Information Security Policy
	9.1.1	Access control policy
	9.4.2	Secure Log-On Procedures
	11.2.8	Unattended user equipment
	11.2.9	Clear desk and clear screen policy
	18.2.2	Compliance with Security Policies and Standards
ISO 27799	7.2.1	Information Security Policy Document
	7.2.2	Review of the Information Security Policy
	7.8.1.2	Access Control Policy
	7.8.3	Unattended User Equipment
	7.8.3	Clear desk and Clear Screen Policy
	7.8.4	Secure Log-On Procedures
	7.8.4	Session Time-Out
	7.8.4	Limitation of Connection Time
	7.12.3	Compliance with Security Policies and Standards
IEC 62443-3-3	SR 2.5	Session Lock
	SR 2.6	Remote session termination

III. Security Argument Pattern

As mentioned, in the previous section, the security case comprises of a security capability argument pattern (throughout the remainder of this paper this will be referred to as a pattern). The pattern has been developed to: 1) reduce the complexity of the security case [16]; 2) reduce the likelihood of incomplete/inadequate arguments; and 3) with the inclusion of this information presented in the security case, it is anticipated that the integrity of the evidence is better understood. Patterns can also support the concept of re-usable arguments that can be recorded and retrieved for re-use within a security case for a particular medical device, or for multiple security cases with similar type risks associated with the design and use of multiple of medical devices. The pattern uses GSN notation and additional extensions as presented in [11].

Fig. 1 provides an overview of the pattern.

- The pattern takes a risk-based approach and starts with a top-level argument claim (C2) addressing a particular security capability, in this example, automatic log off (ALOF). (C2, not C1 is used here as C1 will be the entire security case top level claim. See Section IV).
- The pattern is applied to each of the 19 security capabilities regardless of whether the security capability is required or not. If a particular security capability is not required (C3) justification for non-selection is required (J1).
- Where the security capability is required, the pattern will be developed through C4 with the inclusion of supporting information at CTXT3.
- At this point the strategy of the argument changes to address the identified risks (S1). In order to argue that all *potential* risks are mitigated, J2 should be instantiated to include, or refer to, a risk acceptance policy to justify the choice of risks to receive risk-treatment.
- C5 asserts the completeness of threat/vulnerability identification with CTXT4 instantiated to include the output of this process.
- C6 claims that no unacceptable risks, as defined by the policy at J2, exist.
- Where no unacceptable threats/vulnerabilities exist (n=0), Sn1 is instantiated otherwise, at C7, each of the threats requiring risk treatment are addressed individually.
- Additional information regarding the cause or threat scenario for each individual risk should be detailed and instantiated at CTXT5.

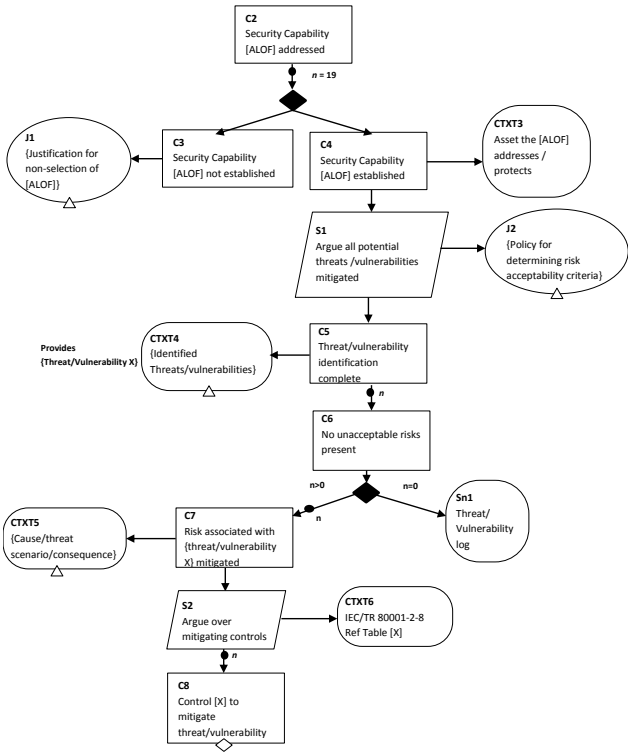

Fig. 1. Security Capability Argument Pattern

- The strategy of the argument changes once again at S2 to argue over the selection of mitigating controls for each of the identified risks requiring risk-treatment.
- CTXT6 should be instantiated with a reference to the source of the security control. In this case IEC/TR 80001-2-8 is included; however, a medical device manufacturer may choose another source or guidance for selection of security controls.
- Finally, at C8 the claim relates to each of the selected security controls.

IV. SECURITY CASE

In support of IEC/TR 80001-2-2 and the security capabilities, development of security cases are the key element of this framework for the interchange of security capability information between medical device manufacturers and healthcare delivery organisations. The purpose of this framework is to provide an end to end solution useful during development, certification and operation.

The pattern (presented in section III) constitutes only a subset of the security case. In addition to the components of the pattern depicted in Fig.1, there are a number of additional components required in order to complete the security case. These include:

- The top-level claim (C1) – This is the overall claim and purpose of the security case which, in this case may be written as "*All security capabilities have been acceptably established"*. C1 is developed to include the underlying patterns for each of the 19 security capabilities;
- Information regarding the medical device, its intended use, operational environment etc. should be included as context (CTXT1) at the top-level claim (C1). This information is valuable in terms of agreements between stakeholders and also to provide information to healthcare delivery organisations for optimal operational use post deployment;
- Context (CTXT2) regarding assets, medical device system description, interfaces, boundaries etc. should also be included in a separate context component at the top-level claim. Again, this information supports ideal operational use;
- Evidence (Sn#) or proof of the successful establishment of a security control. Evidence is the most crucial component of the security case which should be adequate, necessary and suitable [17] (connected to the lowest layer of sub-claims).

Security controls selected by the medical device manufacturers, may often be technical controls and evidence should be documented in the security case to demonstrate confidence in the establishment of those controls. This evidence may include results of testing, analyses or historical information. However, as the intention is to develop a framework that is useable by both manufacturers and healthcare delivery organisations (end users), additional security controls may be required. In order to enable healthcare delivery organisations to maintain the security capability, further administrative or operational controls may be required. For example, consider the security capability "automatic logoff" where a risk of exposure to confidential health data exists without the capability. A medical device manufacturer may select authentication controls by enabling passwords or tokens. The manufacturer may also establish authentication failure handling controls to allow the system to disable after a number of incorrect log-on attempts. Results of tests carried out to ensure these controls have been correctly implemented are documented by the medical device manufacturer as evidence within the security case. In order to support these controls, a healthcare delivery organisation may develop an "authentication and identification" policy, therefore, providing additional evidence to support the establishment of the security capability automatic logoff.

IV. CONCLUSION AND FUTURE WORK

This paper presents a brief overview of ongoing work in the area of medical device security assurance within the Regulated Software Research Centre. The security case framework incorporates a number of existing international standards, guidance documents and processes which have guided the development of the security argument pattern. The security argument pattern has been structured in such a way to provide regulators and healthcare delivery organisations with a comprehensive matrix showing the link between the security risks, associated causes, the mitigating security controls and evidence of those controls being implemented to establish the security capability.

In addition to developing a catalogue of security controls relating to the security capabilities, a vulnerability database is currently being developed. This 'live' database will provide a link between each of the 19 security capabilities, their associated vulnerabilities and mitigating controls. The purpose of this is to develop a security case repository to inform medical devices manufacturers during security risk management activities.

The catalogue of security controls is currently being validated by a working group of international security experts and also experts from the International Standards Committee IEC SC62a. It is expected that this will be published as IEC/TR 80001-2-8. A new work item proposal has also been raised by the authors within the same International Standards Committee to publish a second technical report (TR). This TR, *IEC/TR 80001-2-9 - Application risk management for IT networks incorporating medical devices – Part 2-9: Application guidance – Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities* [18] has recently been drafted and submitted for ballot and comments. The TR presents a framework for developing the security cases to establish confidence in the security capabilities outlined in IEC/TR 80001-2-2.

In terms of developing, interpreting and updating the security cases, the framework will also be validated in

industry both with medical device manufacturers and healthcare delivery organisations located both in Europe and the US.

In the medical device domain, a gap exists as there is no standardised way to assist organisations to satisfy new security related requirements [19]. Therefore, the objective of this research is to investigate this gap further and provide a solution to benefit the following:

- Medical device manufacturers; as they will be soon be required to demonstrate evidence that a medical device is secure both from a development and a final product perspective [1]. One of the main aims of this research is to provide a framework to assist manufacturers to demonstrate and communicate the security capability of medical devices.
- Healthcare delivery organisations; they have been frustrated for years with medical device manufacturers and vendors who refuse to address the security issues that medical devices create in a timely manner [20] [21]. Medical device security is becoming increasingly important for healthcare delivery organisations as they are responsible for the security assurance of devices on their networks [22] [23] [24]. This research addresses the needs of the healthcare delivery organisations through the integration of security cases as part of their on-site risk management process.

At present, there is no formal method for addressing security practices within the medical device industry. This is the primary focus of this research and so it is expected that the output of this research will positively impact the medical device domain in both the EU and the US by building awareness of security vulnerabilities, threats and related risks between the healthcare delivery organisations and medical device manufacturers.

ACKNOWLEDGMENT

This research is supported by the Science Foundation Ireland (SFI) Stokes Lectureship Programme, grant number 07/SK/I1299, the SFI Principal Investigator Programme, grant number 08/IN.1/I2030 (the funding of this project was awarded by Science Foundation Ireland under a co-funding initiative by the Irish Government and European Regional Development Fund), and supported in part by Lero - the Irish Software Engineering Research Centre (http://www.lero.ie) grant 10/CE/I1855.

REFERENCES

1. FDA and CDRH, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, in *Draft Guidance for Industry and Food and Drug Administration Staff*2013.
2. Finnegan, A., F. McCaffery, and G. Coleman, *A Process Assessment Model for Security Assurance of Networked Medical Devices* in *SPICE 2013*2013, Springer: Bremen, Germany. p. 25-36.
3. FDA and CDRH, *Total Product Life Cycle: Infusion Pump - Premarket Notification [510(k)] Submissions - Draft Guidance*, 2010.
4. IEC, *TR 80001-2-2 - Application of risk management for IT-networks incorporating medical devices - Guidance for the disclosure and communication of medical device security needs, risks and controls*, 2011, International Electrotechnical Committee,. p. Page 30.
5. ISO, *EN ISO 27799:2008 Health informatics. Information security management in health using ISO/IEC 27002*, 2008.
6. ISO/IEC, *27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements*, 2005.
7. IEC, *62443-3-3 Ed 1.0 -- Security for industrial automation and control systems -Network and system security -- System security requirements and security assurance levels* 2013.
8. NIST, *800-53 R4 - Recommended Security Controls for Federal Information Systems and Organisations*, U.S.D.o. Commerce, Editor 2013.
9. ISO/IEC, *15408-2 Information Technology - Security Techniques - Evaluation Criteria for IT Security*, in *Security Functional Components*2008.
10. ISO/IEC, *15408-3 Information Technology - Security Techniques - Evaluation Criteria for IT Security*, in *Security Assurance Components*2008.
11. Kelly, T., *Arguing Safety - A Systematic Approach to Managing Safety Cases*, in *Department of Computing*1998, University of York.
12. Kelly, T. and R. Weaver, *The Goal Structuring Notation – A Safety Argument Notation*, 2004.
13. Bloomfield, R. and P. Bishop, *Safety and assurance cases: Past, present and possible future - an Adelard perspective.* 2010.
14. Retrieved 10 May 2014. *http://www.merriam-webster.com/dictionary/defeasible*. defeasible.
15. IEC/WD, *80001-2-8 - Application of risk management for IT networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2. Lead Author: A.Finnegan*, In Press.
16. Yamamoto, S. and Y. Matsuno, *An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case*, in *ASSURE 2013*2013: San Francisco, CA, USA.
17. Zeng, F., M. Lu, and D. Zhong. *Software Safety Certification Framework Based on Safety Case*. in *Internation Conference on Computer Science & Service System (CSSS)*. 2012.
18. IEC/WD, *80001-2-9 - Application of risk management for IT networks incorporating medical devices – Part 2-8: Application guidance - Guidance*

for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities. Lead Author: A.Finnegan, In Press.
19. Government Accountability Office, *Medical Devices, FDA Should Expland Its Consideration of Information Security for Certain Types of Devices*, GAO, Editor 2012.
20. Talbot, T., *Computer Viruses Are "Rampant" on Medical Devices in Hospitals*, M.T. Review, Editor 2012.
21. Millman, G.J., *Medical Device Makers Slow to Address Cyber Risks, Hospitals Complain*, W.S. Journal, Editor 2013.
22. FDA and CDRH, *FDA Safety Communication: Reminder from FDA: Cybersecurity for Networked Medical Devices is a Shared Responsibility*, 2009.
23. DHS, *Attack Surface: Healthcare and Public Heath Sector*. 2012.
24. Deloitte, *Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives.* 2013.